AhnLab

安全月刊

2021.06 Vol.103

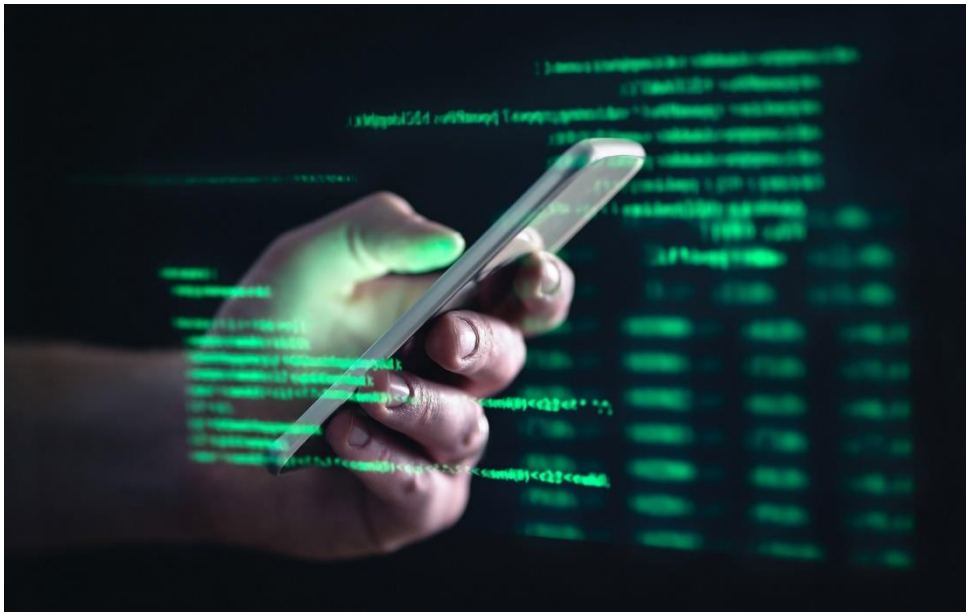
语音钓鱼攻击

语音钓鱼恶意应用趋势报告

不断发展的语音钓鱼攻击，使用恶意应用窃取用户信息

正如多数人所知，语音钓鱼是仅通过电话欺骗受害者以窃取金钱或信息。但是，与其他网络攻击一样，语音钓鱼攻击方法也在不断发展，使用恶意应用程序的频率也随之增加。此类攻击更为复杂，例如在与受害者通话中诱导安装恶意应用程序（以下简称“恶意应用”），并在安装后从受感染的终端收集个人信息。

在本文中，我们将了解语音钓鱼恶意应用程序的攻击手段和防止对策。



据2020年韩国警察厅统计资料，语音钓鱼的受害事例持续增加。截至2020年8月，已确认的受害事例超过2,000起。

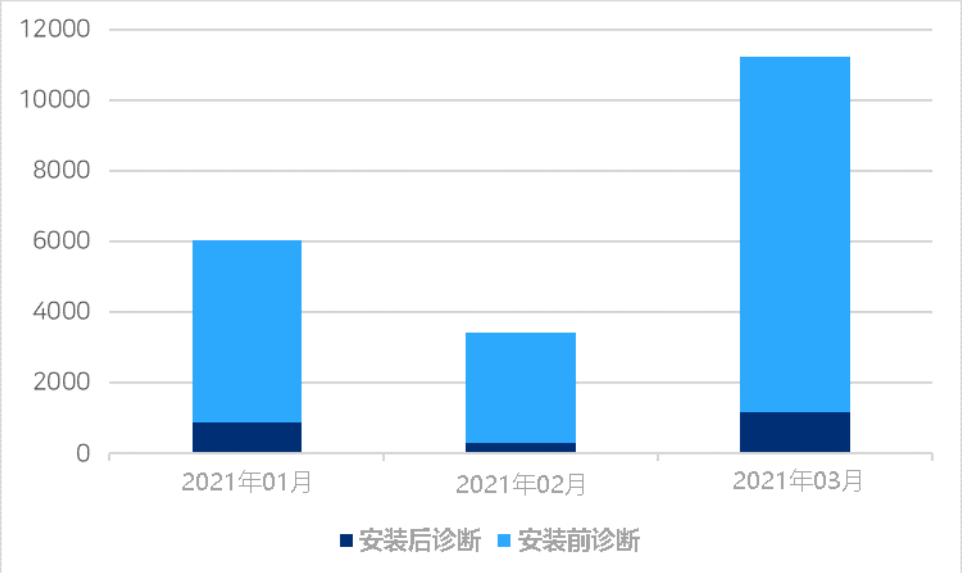
年度	冒充机构的事件数量	冒充机构的受害金额(韩元)	冒充机构的抓获件数	贷款诈骗事件数量	贷款诈骗受害金额(韩元)	贷款诈骗抓获件数
2016	3,384	541亿	3,860	13,656	927亿	7,526
2017	5,685	967亿	3,776	18,574	1,503亿	15,842
2018	6,221	1,430亿	4,673	27,911	2,610亿	25,279
2019	7,219	2,506亿	5,487	30,448	3,892亿	33,791
2020	5,006	1,492亿	2,924	16,008	3,036亿	20,286

【表 1】与语音钓鱼受害相关的韩国警察厅统计资料（数据来源：https://www.data.go.kr/en/index.do）

值得关注的是， 利用恶意应用的进行语音钓鱼正在逐渐增加。这种变化估计在提高语音钓鱼成功率方面起到了很大作用。

AhnLab对2021年第一季度收集的5,527个恶意应用的应用标签进行了分析， 发现5,397个是伪装成金融机构进行贷款诈骗的恶意应用，159个是冒充检察厅等国家机构的恶意应用。

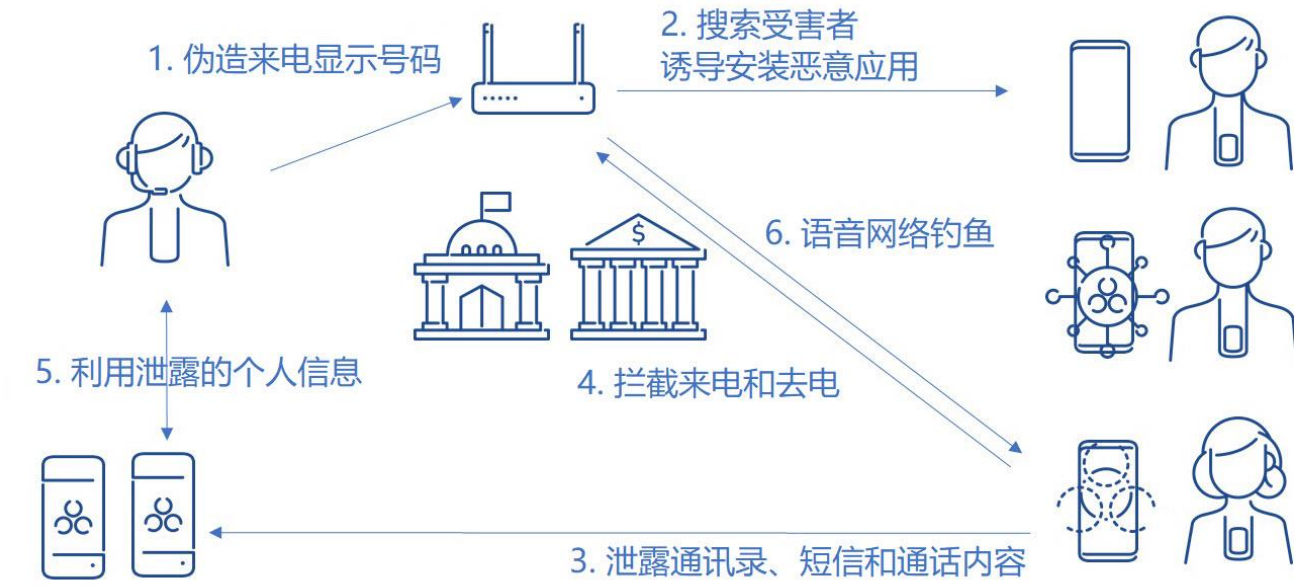
此外，下载或安装语音钓鱼应用的事例也在持续增加。【图 1】是基于V3 Mobile收集的诊断日志，对安装语音钓鱼恶意应用前后的诊断情况进行的分析。今年第一季度 ， 共诊断出20,720个语音钓鱼恶意应用。其中 ，18,392个在安装前的下载阶段被诊断为恶意应用，2,328个在安装后被诊断为恶意应用。



【图 1】语音钓鱼应用感染情况

语音钓鱼的攻击手段

通常， 大多数的人认为语音钓鱼就是通过打电话来欺骗受害者以获取金钱上的利益。但近年来， 攻击手段进一步升级， 例如通过与受害者通话诱导安装恶意应用， 安装后从受感染的终端收集个人信息等。此外， 它似乎通过使用各种方法来提供语音钓鱼的成功率，例如监视受害者的通话和短信，拦截来电和去电。

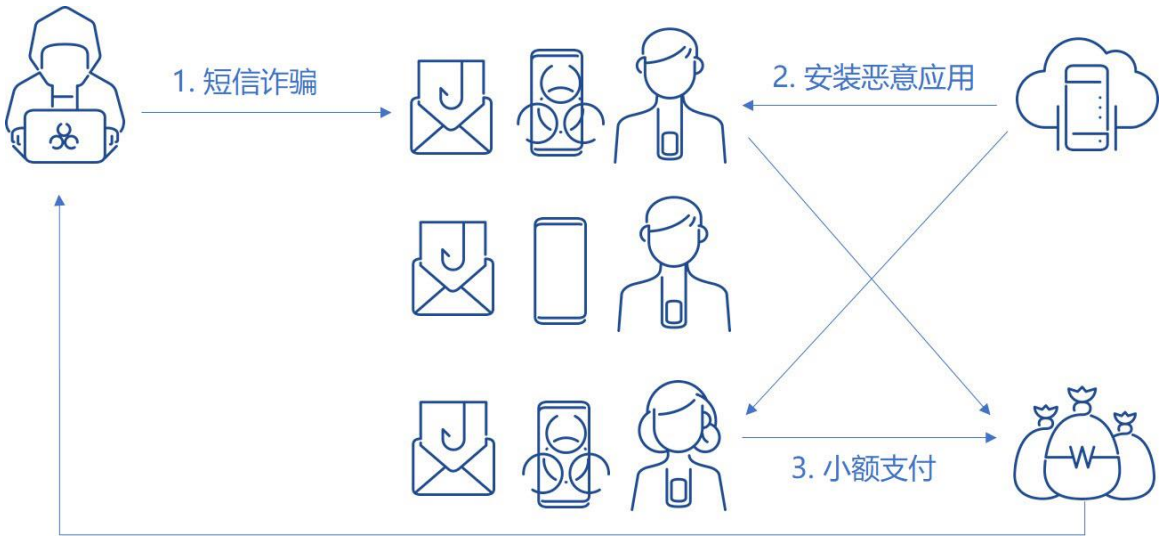


【图 2】语音钓鱼恶意应用的攻击结构图

首先，语音钓鱼诈骗犯利用来电显示号码修改软件隐藏来电号码是海外电话，并冒充贷款广告给受害者拨打电话以欺骗受害者。然后，他还会要求受害者通过手机通讯软件或短信（SMS）等收到的链接下载并安装恶意应用。如果受害者受骗并安装了恶意应用， 则存储在手机的信息 （例如短信内容、联系人信息、通话记录和已安装应用等）将传送到黑客的C&C服务器。

语音钓鱼诈骗犯通过安装的恶意应用， 可以从受害者哪里获取大量的短信内容、联系人等个人信息， 并在与受害者通话时利用这些信息来获取信任。此外， 通过利用恶意应用篡改来电显示， 来自诈骗犯的电话被伪装成来自国家机构或者金融机构的电话。当受害者给这些机构拨打电话时， 他们会将电话转到语音钓鱼诈骗犯， 以免被受害者怀疑。

这种针对特定受害者分发恶意应用不同与分发相同的恶意应用给非特定人群并拦截小额支付短信的短信诈骗恶意应用。



【图 3】短信诈骗恶意应用攻击结构图

短信诈骗恶意应用通过与日常生活相关的链接（例如周岁宴、请柬等）诱导受害者安装相同的应用。安装的恶意应用通过从C&C服务器收到的命令，攻击小额支付系统中的漏洞，从多数受害者那里获取小额资金。

由于短信诈骗恶意应用使用同一应用给多数受害者造成损害，因此它的生命周期相对较短。而语音钓鱼恶意应用通常会先确保少数的受害者后，再分发个人定制的恶意应用，因此在受害者进行举报之前，很难确保相关应用的信息。

此外，在分发之前，恶意应用制作者会利用韩国智能手机用户经常使用的杀毒应用确认是否被检测到，只有在未检测到的情况下，才分发应用。在这种情况下，即使是已知类型的恶意应用，如果智能手机用户没有启用实时监控功能，则无法被检测到。

举个代表性的例子，有一款名为Kaishi（Android-Trojan/Kaishi）的应用用于语音钓鱼攻击，从2014年初开始不断被发现。

当用户拨入或拨打金融服务相关的电话号码时，Kaishi会通过将其更改为攻击者所需的号码来连接通话。它主要冒充金融银行应用，也冒充知名应用，例如Google Play 、Chrome和Flash Player等。另外，冒充公共机构和金融相关机构的情况也不少见。虽然具有相同的伪造通话的功能，但Kaishi似乎在不断地进行管理，内部实现方式发生了变化。

尤其，当冒充金融公司A的应用被发送到内部监视的特定电话号码（例如金融服务客户咨询电话、贷款咨询电话、检察厅电话等）或从其接收时，会拦截该通话并将其转发到最初存储在恶意应用中的电话号码或从C&C服务器获取的特定电话号码。而且，在屏幕上显示看起来是正常的并未更改的号码。此应用具有向服务器传送短信、通话记录和通讯录信息的功能。

如何防止语音钓鱼攻击?

为了防止语音钓鱼攻击，需要屏蔽诈骗犯使用的电话号码和C&C服务器以及分发服务器。此外，如果能够快速确保恶意应用，则可以在安装于终端的应用中找出语音钓鱼应用。还可以考虑通过确认通话内容来辨别语音钓鱼并通知用户的方法。

垃圾号码检测应用可以通过用户的举报，掌握用于语音钓鱼的电话号码，并防止后续损害。像V3 Mobile之类的杀毒应用可以快速确保和诊断恶意应用，防止同一类型的恶意应用造成的损害扩散。另外，可以通过分析已确保的应用并与相关机构共享C&C服务器来阻止访问。最近，在掌握了语音钓鱼通话之后，通过机器学习技术，分析来电者的口音或通话内容。

但是，由于语音钓鱼通过指定受害者来诱导安装应用的特性，因此必须在在受害者认知受害之后，才能确保用于攻击的电话号码、分发URL以及应用。

语音钓鱼诈骗犯在拨打电话时，可能通过来电显示号码更改软件利用在垃圾号码检测应用中未确保的电话号码，或通过任意篡改电话号码评分绕过垃圾号码检测应用。以这种方法接近受害者后，提供在韩国国内广泛使用的安全应用无法检测到的恶意应用，以此迂回检测。即使屏蔽通过受害者的举报而确保的语音钓鱼的电话号码、分发URL、恶意应用和C&C服务器，页不容易提前屏蔽，因为语音钓鱼诈骗犯在一旦得知被曝光便会更改应用和过去信息。

对于通过实时分析通话内容来警告语音钓鱼的安全应用，从Android 9.0 Pie开始，通过第三方应用进行通话录音API的访问被屏蔽，在一些终端很难通过分析通话内容来检测到语音钓鱼。

对于安全企业，如果能收集在终端上安装的应用中通过非官方渠道安装的应用，则可以快速作出响应。但是，考虑到个人信息保护法和著作权保护，很难收集安装在个人终端上的应用。

综上所述，除了各机构和安全企业为防止和阻止语音钓鱼和恶意应用做出努力，用户也应该要认识到其局限性，并有必要采取自我保护的态度。

首先，对于通过通话来要求提供个人信息时，应该予以拒绝。而且，应该要避免安装以未知路径分发的应用，并通过官方渠道来安装应用。此外，利用垃圾号码检测应用确认接收的电话或短信的可信度，将有助于防止语音钓鱼攻击的损害。

最后，需要使用V3 Mobile定期检查是否安装了恶意应用。作为参考，AhnLab对2021年第一季度收集的诊断日志进行了分析，确认语音钓鱼应用数理为 20,720个，其中除了2,328个以外，均是在下载过程中被诊断出来

的。另外，对于安装后诊断出的恶意应用，可以在安装后的短时间内进行诊断，因此可以将损失降到最低。

诊断文件

Android-Trojan/Kaishi.f7572

Android-Trojan/Kaishi.f733c

Android-Trojan/Kaishi.f72b5

Android-Trojan/Kaishi.f509d

相关IoC

HASH

76431d668e750e0ee47242bbda5252cc

C&C服务器

154.83.102.138

112.121.161.190

112.121.161.186 ~ 9

AhnLab

安全月刊

https:// cn.ahnlab.com

https://global.ahnlab.com

https://www.ahnlab.com

关于AhnLab

Ahnlab的尖端技术和服务不断满足当今世界日新月异的安全需求，
确保我们客户的业务连续性，并致力于为所有客户打造一个安全的计算环境。
我们提供全方位的安全阵容，包括经过证实的适用于桌面和服务器的世界级防病毒产品、
移动安全产品、网上交易安全产品、网络安全设备以及咨询服务。
AhnLab已经牢固地确立了其市场地位，其销售伙伴遍布全球许多国家和地区。

AhnLab

北京市朝阳区望京阜通东大街1号望京SOHO塔2 B座 220502室 | 上海市闵行区万源路2158号18幢泓毅大厦1201室
电话：+86 10 8260 0932（北京） / +86 21 6095 6780（上海） | cn.sales@ahnlab.com